Tier 1 Control Standards (State-Wide)

Confidential System Architecture

Standard ID
IOT-CS-ARC-001

Published Date
9/1/2016

Effective Date
9/1/2016

Last Updated
3/8/2017

Next Review Date
3/8/2018

Policy
06.0 Access Control (PR.AC)
06.5 PR.AC-5
06.5.1 Network Segmentation

Purpose
Isolating critical systems will reduce opportunities for unauthorized access and contain possible incidents or breaches.

Scope
IOT Supported Entities

Statement
The State's Protected Zone (PZ) serves as a mechanism to isolate confidential systems. Confidential systems shall follow the requirements listed below:

General:

Access, Isolation, and Communication:

- No file sharing access between zones (must use IOT's 'Manage File Transfer Solution')
- Information System tiers must not span Zones
- All network traffic shall be denied by default. Only allow the hosts, ports, and services that are explicitly required and all entry points shall be limited based on least functionality
- Cannot connect to and therefore negatively impact any other agency without Memorandum of understanding (MOU). Further, cannot lessen the security of an agency application in the PZ, without formal risk acceptance by appropriate parties within the agency (MIS Director or above).
- Information System(s) must consist of a production and non-production domain (environment)
- Production and non-production domains cannot be bridged unless there is an IOT approved change control process in place
- Confidential, private and/or sensitive data shall follow State standards per domain

Legacy system's shall follow these additional requirements:

- Must be isolated behind the Protected Zone firewall into agency's dedicated VLAN for legacy systems, and not comingled with "New and Upgraded Systems" portion of the zone

- No connection to external shared services outside the PZ (e.g., SQL Reporting Server, Shared Internet Information Server (IIS), Shared Oracle)
- Must not communicate outside the agency PZ VLAN to another information system belonging to the same agency without risk acceptance

New and Upgraded Systems* shall follow these additional requirements:

- Information System(s) shall be partitioned into a three-tier architecture that consists of a presentation, application and a database tier where one VLAN is used for each tier per domain
- Application Development must adhere to three tier architecture, secure application development (DISA APPLICATION SECURITY AND DEVELOPMENT) and follow SDLC process.

System Hardening

All systems must utilize IOT's secure baseline configuration

- All server operating system(s)
- Database Server/Instances
- System components and features (e.g., .NET, IIS)
- Shall follow IOT's Architecture Logging Standard and send both audit and application logs to enterprise SIEM
- All components must utilize IOT's management infrastructure (e.g, AD services, NTP, DNS, Netbackup, software update services)
- Security controls shall be enabled to the level commensurate with the system classification (e.g., confidential)

Access, Isolation and Communication

- No direct user access to servers in any tier in the protected zone; Administrative connections to servers in the Protected Zone must be through an approved IOT Solution (e.g., Citrix) and no remote connections over Virtual Private Network (VPN)
- Agencies shall not use VPN, wireless or tunneling access to any protected zone environment. Must utilize protected zone stateful inspection/application firewall hardware and software
- Communication between zones and tiers must be encrypted following IOT's Data Encryption Standard
- Interconnection between information systems that are in different zones must go through IOT application or web gateway
- Web servers shall be placed in a presentation tier (DMZ) Virtual Local Area Network (VLAN) allocated by IOT
- External network connection shall connect only through IOT's application gateway or approved proxy services and public access into the State's network shall be denied except for approved communication through IOT's application/proxy and PZ firewall
- Agencies shall not use VLANs between confidential tiers and any other network of a lower security level without traversing through a DMZ and proxy

Administration

Boundary Protection

- All communication shall pass through a double hop authentication method when remotely accessing the secure environment. Double hop is two IOT managed devices connecting between different security zones. Remote access is defined as any network that is not controlled or managed by IOT or viewed as untrusted.
- Remote access first hop authentication must happen at a centralized point prior to gaining access to the State network
- Internal access second hop authentication must happen at centralized point prior to gaining access to the protected zone (PZ)
- Protects boundaries from any data exfiltration between client and protected application or database. All user initiated data/files in or out of the secure environment shall go through IOT's Manage File Transfer Solution

- All systems that make up the second hop shall be isolated and hardened to Confidential System Architecture Standards
- Utilize IOT's centrally managed on premise access solution, isolated per security zone and then per security domain(environment), which uses a trusted operating system and enforces IOT's approved security policy
- Provide application firewall proxy services to intercept arriving traffic on behalf of the destination, examine application payload, and then relay permitted traffic to the destination

Encryption

- All in-transit communications must be encrypted

Logging

- Shall follow IOT's Architecture Logging Standard and send both audit and application logs to enterprise SIEM

Least Privilege

- IOT's Multi-factor Authentication (MFA) will be required on the initial connection and prior to transitioning from any State network zone
- Active Directory integrated and utilize role based permission groups for the following roles:
  - IOT administration
  - Agency administration
  - Vendor/Consultant administration
  - Accounts used to administer confidential systems are privileged accounts only

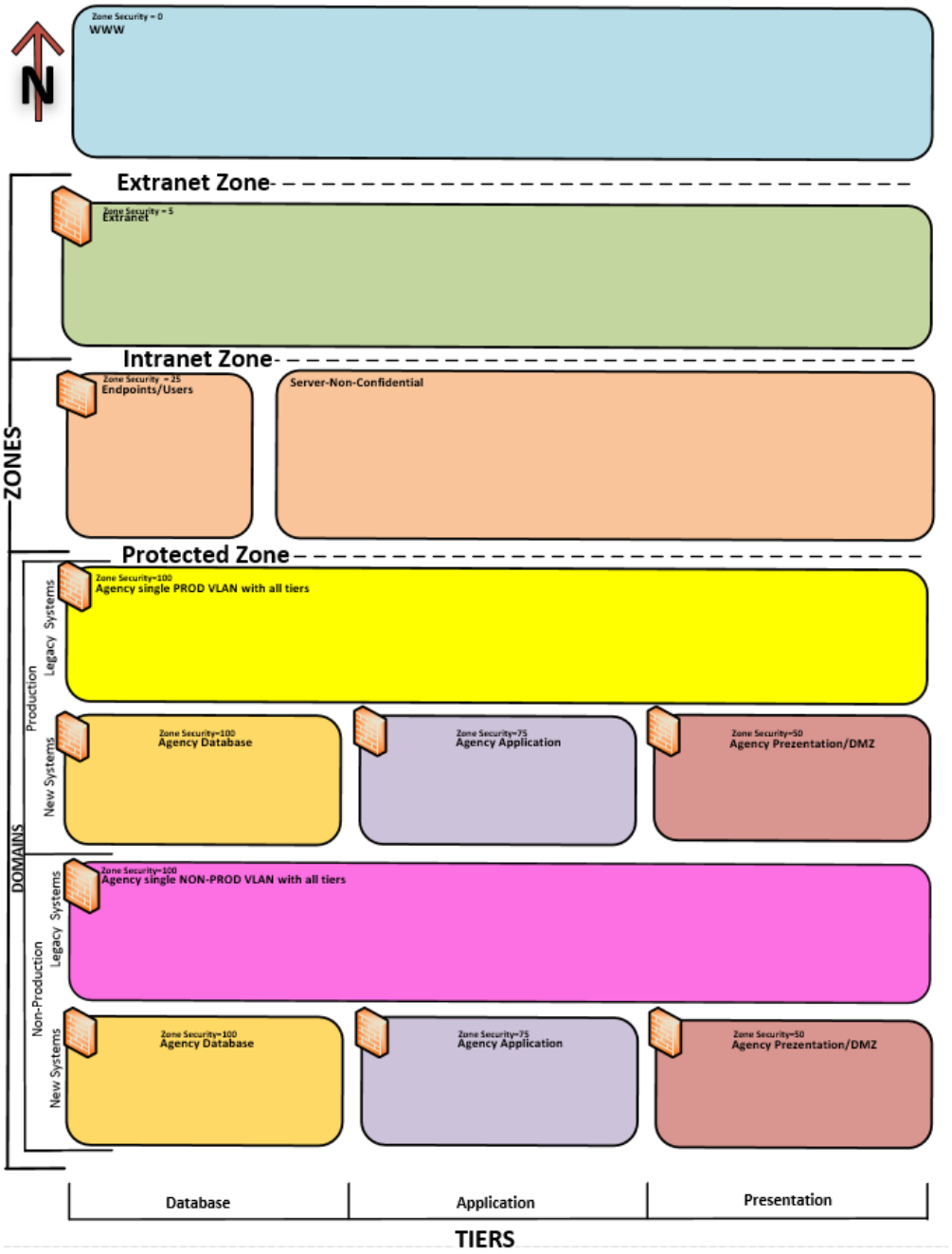

Figure 1: Example of Agency Protected Zone Architecture

Roles

Information Asset Owners/System Owners

Responsibilities

Information Asset Owners/System Owners must work with Agency Management to determine what systems are required to be in the Protected Zone and appropriately configure them to maximize security while conserving required functionality. IOT shall work with agencies to architect the systems that meet the State's security requirements.

Management Commitment
Management shall ensure that all confidential systems are segmented appropriately.

Coordination Among Organizational Entities
Agencies shall coordinate with the IOT Architecture team for placing the system in the PZ.

Compliance
Agencies shall review the Information Systems Inventory (ISI), the authoritative source of system information to understand all confidential systems related to their agency. All confidential systems must be appropriately isolated.

Exceptions
Exceptions will be handled on a case by case basis through the Director of Risk & Compliance, State CISO and the IOT Architecture team.